PTO/SB/08a (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. KOCHER
Art Unit	2132
Examiner Name	Abdulhakim NOBAHAR
Attorney Docket Number	44424162-8721

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/H.N./	2M	US-6,070,795	06-06-2000	Feiken	
/H.N./	2N	US-6,247,129	06-12-2001	Krathleg et al.	
/H.N./	2O	US-6,393,567	05-21-2002	Colnot	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
/H.N./	2P	WO 97/14085	04-17-1997	British Telecommunications Public Limited Company		
/H.N./	2Q	WO 97/14086	04-17-1997	British Telecommunications Public Limited Company		

Examiner Signature	/Abdulhakim Nobahar/	Date Considered	06/11/2007

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. KOCHER
Group Art Unit	2132
Examiner Name	Nobahar, Abdulhakim
Attorney Docket No.	44424162-8721

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	2J	United States Air Force Audio Visual Presentation, "So You Think You're Secure", Aerospace Audio Visual Service; TF32-4599, 1972; Military Airlift Command; TF 6502.	
/H.N./	2K	Cryptography Research Inc. v. VISA International Service Association, VISA International Service Association's Answer to Second Amended Complaint and Counterclaims, United States District Court Case No. C 04-04143 JW (HRL), Northern District of California, San Jose Division, April 23, 2007.	
/H.N./	2L	Cryptography Research Inc. v. VISA International Service Association, Defendant VISA International Service Association's Final Invalidity Contentions for U.S. Patent No. 6,327,661 Pursuant to Patent L.R. 3-6(B), United States District Court Case No. 5:04-CV--04143-JW (HRL), Northern District of California, San Jose Division, December 8, 2006.	

Examiner Signature	/Abdulhakim Nobahar/	Date Considered	06/11/2007

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 3

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. KOCHER
Art Unit	2132
Examiner Name	Nobahar, Abdulhakim
Attorney Docket Number	44424162-8721

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/H.N./	1A	US-4,225,962 B1	09-30-1980	Meyr et al.	
	1B	US-4,669,117 B1	05-26-1987	Van Eck	
	1C	US-4,932,057 B1	06-05-1990	Kolbert	
	1D	US-4,937,866 B1	06-26-1990	Crowther et al.	
	1E	US-5,068,894 B1	11/26/1991	Hoppe	
	1F	US-5,086,467 B1	02-04-1992	Malek	
	1G	US-5,157,725 B1	10-20-1992	Lindholm	
	1H	US-5,165,098 B1	11-17-1992	Hoivik	
	1I	US-5,181,243 B1	01-19-1993	Saltwick et al.	
	1J	US-5,216,713 B1	06-01-1993	Lindholm	
	1K	US-5,249,294 B1	09-28-1993	Griffin, III et al.	
	1L	US-5,477,039 B1	12-19-1995	Lisimaque et al.	
/H.N./	1M	US-5,944,917 B1	11-30-1999	Wuidart	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
/H.N./	1N	EP 0 452 031 A2	10-16-1991	Ferranti International		☐
/H.N./	1O	EP 0 563 912 A1	10-06-1993	Data Protection S.R.L.		☐
/H.N./	1P	JP 10-197610	07-31-1998	Sony Corp		☐
/H.N./	1Q	JP 10-084223	03-31-1998	Mitsubishi Electric Corp.		☐
/H.N./	1R	JP 62-260406	11-12-1987	Nippon Electric Co.		☐
/H.N./	1S	JP 62-082702	04-16-1987	Hewlett-Packard Yokogawa		☐
						☐

Examiner Signature	/Abdulhakim Nobahar/	Date Considered	06/11/2007

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 3

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. KOCHER
Group Art Unit	2132
Examiner Name	Nobahar, Abdulhakim
Attorney Docket No.	44424162-8721

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/H.N./	1T	ANDERSON, Ross et al., "Tamper Resistance - a Cautionary Note", The Second USENIX Workshop on Electronic Commerce Proceedings, Nov. 18-21, 1996, Oakland, CA.	
/H.N./	1U	CHAUM and Price (Eds.), "IC Cards in High-Security Applications", Advances in Cryptology - Eurocrypt '87, LNCS 304, Amsterdam, NE (1988), pp. 177-199.	
	1V	GOUTAY, J., "Smart Card Applications in Security and Data Protection", Advances in Cryptology - Eurocrypt '84; LNCS 209, Springer-Verlag, Berlin, Germany; (1985) pp. 459-463.	
	1W	GUILLOU, L.C. et al., "Smart Card, a Highly Reliable and Portable Security Device", Advances in Cryptology - CRYPTO '86; LNCS 263, Springer-Verlag, Berlin, Germany; (1987) pp. 464-479.	
	1X	GUILLOU, L.C., "Smart Cards and Conditional Access", Advances in Cryptology - Eurocrypt '84; LNCS 209, Springer-Verlag, Berlin, Germany; (1985) pp. 480-489.	
	1Y	GUTHERY, Scott, "Smart Cards", www.usenix.org/publications/login/1989-5/guthery.html; May, 1989.	
	1Z	HIGHLAND, Harold Joseph, "The Tempest over Leaking Computers", Abacus, Vol. 5(2), Winter 1988, pp. 10-18, 53. http://cryptome.org/tempest-leak.htm	
	2A	ISO/IEC 7816 International Standard, Geneva, CH: Part 1 Physical Characteristics (Ref. No. ISO/IEC 7816-1:1998(E)), Part 1 Amendment Physical Characteristics (Ref. No. ISO/IEC 7816-1:1998/AMD.1:2003(E)), Part 2 Dimensions and Location of the Contacts (Ref. No. ISO/IEC 7816-2:1999(E)).	

Examiner Signature	/Abdulhakim Nobahar/	Date Considered	06/11/2007

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 3 of 3

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. KOCHER
Group Art Unit	2132
Examiner Name	Nobahar, Abdulhakim
Attorney Docket No.	44424162-8721

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	2B	KRIVACHY, T., "The Chipcard - An Identification Card with Cryptographic Protection", Advances in Cryptology - Eurocrypt '85; LNCS 219, Springer-Verlag, Berlin, Germany (1986) pp. 200-207.	
	2C	KUHN, Markus G. et al., "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations", Second Workshop on Information Hiding, Portland, Oregon, April 15-17, 1998.	
	2D	MENZES, A.J. et al., Handbook of Applied Cryptography, Chapters 1, 5 and 7; CRC Press, Boca Raton; Florida (1997).	
	2E	MEYER, Carl H. et al., Cryptography - A New Dimension in Computer Data Security; Ch. 1; John Wiley & Sons, 1982.	
	2F	RANKL et al., Smart Card Handbook, John Wiley & Sons Ltd., 1997, Chs. 2, 3, 8, 13, and pages 84-89, Chichester, England.	
	2G	SCHMIDT, Dick, "Visions on Development in Information Security", TNO Conference, Delft, Netherlands, October 2-3, 1997.	
	2H	SMULDERS, Peter, "The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables", Computers and Security, Vol. 9, pp. 53-58, 1990; Elsevier Science Publishers Ltd.	
	2I	WAKERLY, John F., "Introduction to Computers and Programming", Microcomputer Architecture and Programming: The 68000 Family, John Wiley & Sons, New York, N.Y. (1989), Chapter 1, pp 1-16.	

Examiner Signature	/Abdulhakim Nobahar/	Date Considered	06/11/2007

06/11/2007

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 4

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Art Unit	2132
Examiner Name	Nobahar, Abdulhakim
Attorney Docket Number	44424162-8721

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/H.N./		US- 5,412,730	05-02-1995	Jones	
/H.N./		US- 5,483,598	01-09-1996	Kaufman et al.	
/H.N./		US- 5,764,766	06-09-1998	Spratte	
		US- 5,946,397	08-31-1999	M'Raihi et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
/H.N./		WO 97/13342	04-10-1997	GEM-PLUS S.C.A.		
/H.N./		WO 98/52319	11-19-1998	Yeda Research and Development Co.		

Examiner Signature	/Abdulhakim Nobahar/	Date Considered	06/11/2007

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 4

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Art Unit	2132
Examiner Name	Nobahar, Abdulhakim
Attorney Docket Number	44424162-8721

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/H.N./		"Announce: Timing Cryptanalysis of RSA, DH, DSS", sci.crypt newsgroup postings, 13-15 December 1995.	
		"Digital Signature Standard (DSS)", Federal Information Processing Standards Publication 186, 19 May 1994, downloaded: 22 January 2007, website: http://www.itl.nist.gov/fipspubs/fip186.htm	
		"EUROCRYPT '97 Rump Session Program", May 13, 1997, Konstanz, Germany, downloaded: 29 January 2007, website: http://www.iacr.org/conferences/ec97/rump.html	
		"Kocher Algorithm", sci.crypt newsgroup postings, Google Groupes, 12 March 1996, http://groups.google.fr/group/sci.crypt/browse_thread/thread/240f02445602362e/644d5300cdbbf7e3?lnk=gst&q=%q=%22Kocher+Algorithm%22&mum=1&ht=fr#644d5300cdbbf7e3	
		"Public-Key-Algorithm for Digital Signature", National Institute of Standards and Technology, August 1991, pp. 553-564 (German translation).	
		ANDERSON et al., "Robustness Principles for Public Key Protocals", LNCS 963, Proc. Crypto '95, 1995, pp. 236-247.	
		ANDERSON, Ross, "Two Remarks on Public Key Cryptology", Computer Laboratory, University of Cambridge, Technical Report, Number 549, December 2002, ISSN 1476-2986.	
		BEKER et al., "Key Management for Secure Electronic Funds Transfer In a Retail Environment", Proc. Crypto '84, Springer-Verlag, 1998, pp. 401-410.	
↓		BONEH et al., "On the Importance of Eliminating Errors in Cryptographic Computations", Journal of Cryptology, 2001, Vol. 14, No. 2, pp. 101-119.	
/H.N./		BOVELANDER, Ernst, "Smart Card Security 'How Can We Be So Sure?'", COSIC '97 Course, Incs 1528, Springer-Verlag, 1998, pp. 333-337.	

Examiner Signature	/Abdulhakim Nobahar/	Date Considered	06/11/2007

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 4

Complete if Known	
Application Number	10,005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Art Unit	2132
Examiner Name	Nobahar, Abdulhakim
Attorney Docket Number	44424162-8721

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/H.N./		BURMESTER et al., "A Secure and Efficient Conference Key Distribution System", LNCS 1189, Proc. International Workshop on Security Protocols, 1996, Springer-Verlag, 1998, pp. 275-286.	
		DAEMEN, Joan, "Management of Secret Keys: Dynamic Key Handling", LNCS 1528, Proc. COSIC '97 Course, Springer-Verlag, 1998, pp. 264-276.	
		FRANKEL et al., "Proactive RSA", Sandia Report SAND96-0856, April 15, 1996.	
		GENNARO et al., "Robust Threshold DSS Signatures", LNCS 1070, Proc. Eurocrypt '96, Springer-Verlag, 1998, pp. 354-371.	
		GILLOGLY et al., "Notes on Crypto '95 Invited Talks by R. Morris and A. Shamir", Cipher 9, 18 September 1995, http://www.ieee-security.org/cipher/confreports/conf-rep-Crypto95.html	
		HERZBERG et al., "Proactive Secret Sharing Or: How to Cope with Perpetual Leakage", LNCS 963, Proc. Crypto '95, Springer-Verlag, 1998, pp. 339-352.	
		JABLON, David P., "Strong Password-Only Authenticated Key Exchange", Computer Communication Review, September 25, 1996, Vol. 26, No. 5, pp. 5-26.	
		KOCHER, P., Message: "Re: Timing cryptanalysis of RSA, DH, DSS (Tomazic, RISKS 17.59", The Risks Digest, Forum on Risks to the Public in Computers and Related Systems, Volume 17: Issue 60, 3 January 1996, downloaded: 23 January 2007, website: http://catless.ncl.ac.uk/Risks/17.60.html	
		MATSUMOTO et al., "Speeding Up Secret Computations with Insecure Auxiliary Devices", LNCS 403, Proc. Crypto '88, Springer-Verlag, 1998, pp. 499-506.	
/H.N./		NACCACHE et al., "Can D.S.A. be Improved?" -Complexity Trade-Offs with the Digital Signature Standard-", LNCS 950, Proc. Eurocrypt '94, 1995, Springer-Verlag, 1998, pp. 77-85.	

Examiner Signature	/Abdulhakim Nobahar/	Date Considered	06/11/2007

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 4

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Art Unit	2132
Examiner Name	Nobahar, Abdulhakim
Attorney Docket Number	44424162-8721

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/H.N./		NACCACHE, David, "Can O.S.S. be Repaired?" - Proposal for a New Practial Signature Scheme-", LNCS 765, Proc. Eurocrypt '93, 1994, Springer-Verlag, 1998, pp. 233-239.	
		NACCACHE, David, "To Whom it May Concern", Forensic Expert Witness by the Court of Appeal, Paris, 6 December 2006.	
		QUISQUATER et al., "Fast Decipherment Algorithm for RSA Public-Key Crypptosystem", 27th August 1982, Electronics Letters 14th October 1982, Vol. 18, No. 21, pp. 905-907.	
		RANKL et al., "Smart Card Handbook", John Wiley & Sons Ltd., 1997, pp. 66-83, 182-189, 208-217, and 237-272.	
		ROBSHAW et al., "Overview of Elliptic Curve Cryptosystems", RSA Laboratories Technical Note, revised June 27, 1997, downloaded: 23 January 2007, website: http://www.rsasecurity.com/rsalabs/node.asp?id=2013	
		SCHNEIER, Bruce, "Applied Cryptography", 2nd Edition, John Wiley & Sons, Inc., 1996, pp. 525-573 (German translation).	
		SCHNORR, C.P., "Efficient Signature Generation by Smart Cards", Journal of Cryptology, 1991, pp. 161-174.	
		SHAMIR, Adi, "On the Poser of Commutativity in Cryptography", LNCS 85, Proc. 7th Colloquia on Automata, Languages and Programming, 1980, pp. 582-595.	
↓		STEINER et al., "Diffie-Hellman Key Distribution Extended to Group Communication", Third ACM Conf. Computer and Comm. Security, March 1996, pp. 31-37.	
/H.N./		YEN et al., "RSA Speedup with Chinese Remainder Theorem Immune against Hardware Fault Cryptanalysis", IEEE Transactions on Computers, April 2003, Vol. 52, No. 4., pp. 461-472.	

Examiner Signature	/Abdulhakim Nobahar/	Date Considered	06/11/2007

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.